19. SAFETY AND SECURITY

BASIC REQUIREMENT

Under the safety authority provisions of the Federal transit laws, the Secretary has the authority to investigate the operations of the grantee for any conditions that appear to create a serious hazard of death or injury, especially to patrons of the transit service.

As recipients of Urbanized Area Formula Grant Program funds, grantees must annually certify that they are spending at least one percent of such funds for transit security projects or that such expenditures for security systems are not necessary.

FTA and the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) have developed a list of 17 Security and Emergency Management Action Items for Transit Agencies. The action items aim to elevate security readiness throughout the public transportation industry by establishing baseline measures that transit agencies should employ.

The goal of FTA's Safety and Security Program is to achieve the highest practical level of safety and security in all modes of transit. To this end, FTA continuously promotes the awareness of safety and security throughout the transit community by establishing programs to collect and disseminate information on safety/security concepts and practices. In addition, FTA develops guidelines that transit systems can apply in the design of their procedures and by which to compare local actions. Many of the questions in this review area are designed to determine what efforts grantees have made to develop and implement safety, security, and emergency management plans. While there may not be specific requirements associated with all of the questions, grantees are encouraged to implement the plans, procedures, and programs referenced in these questions. For this reason, findings in this area will most often result in advisory comments rather than deficiencies.

AREAS TO BE EXAMINED
1. *Safety*

2. *Security and Emergency Management*

REFERENCES
1. 49 USC Chapter 53, Federal Transit Act, Section 5307(d)(1), Security Expenditures

2. 49 CFR Part 630, "Uniform System of Accounts and Records and Reporting"

3. 49 CFR Part 659, "Rail Fixed Guideway Systems, State Safety Oversight"

USEFUL WEBLINKS
FTA Bus Safety Website

FTA Rail Safety Website

Manual for the Development of Bus Transit System Safety Program Plans

FTA Dear Colleague Letter June 26, 2009

FTA Dear Colleague Letter September 22, 2009

FTA Dear Colleague Letter July 14, 2009

FTA Transit Security Website

TSA BASE

TSA/FTA Action Item

Transit Watch

The Public Transportation System Security and Emergency Preparedness Planning Guide

National Incident Management System

National Response Framework

QUESTIONS FOR THE REVIEW

Part A. Safety

1. *Does the grantee have a written policy on safety? Is it signed by the CEO?*

2. *Does the grantee have a written system safety program plan (SSPP) for its transit services? Does the SSPP address management of the safety function?*

3. *How is the safety function managed? Are there staff safety personnel? If so, are responsibilities and authorities clear? To whom do they report?*

EXPLANATION
FTA is concerned about the safety of both transit passengers and workers. FTA can conduct safety investigations when conditions of any facility, equipment, or manner of operation appear to create a serious hazard of death or injury. These questions are intended to provide an overall understanding of how safety is incorporated into the organization, what kind of emphasis is placed on safety, how the safety program is managed, and how various responsibilities are communicated to personnel at all levels.

Recognizing that safety is an integral part of transit operations, grantees are encouraged to have a written safety policy and safety plan. The safety plan should assign responsibilities for safety management from the most senior executive to the first-line supervisory level. Endorsement by the CEO conveys this importance. At a minimum, a grantee's safety plan should address compliance with applicable legal requirements. Striving for continual improvement to achieve a high level of safety performance should be a program goal. Guidance on the development of a written bus transit system safety program plan is available in an APTA publication entitled, *Manual for the Development of Bus Transit System Safety Program Plans* (1998). Note that the grantee may have a safety plan developed from another source, which responds to specific state or local requirements.

REFERENCE
Manual for the Development of Bus Transit System Safety Program Plans

SOURCES OF INFORMATION
The reviewer will examine the written safety policy or system safety program plan during the site visit. The reviewer will discuss with the grantee the reporting relationships in regard to safety to ensure that the safety function is managed adequately.

DETERMINATION
If the grantee does not have a safety policy or safety plan, an advisory comment is made.

If the safety plan does not address the management of the safety function, if staff responsibilities are not clearly delineated, or the CEO has not signed it, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to prepare a written safety policy or system safety program plan.

The grantee will be advised to revise the plan to adequately address management of the safety function.

4. *What are the investigation procedures for major incidents? What circumstances and conditions determine which incidents will be investigated? Who does the investigation? To whom do reports go? What follow-up action is taken and by whom?*

5. *What key safety issues have been identified and how are they being addressed? Is there an established joint labor/management safety committee that meets on a regular basis, with minutes of the meetings?*

6. *Is there a process for hazard identification and resolution? Are employees encouraged to report potential hazards? When corrective action is needed, how is it initiated and followed up?*

EXPLANATION
Safety issues include more than vehicle and passenger accidents and workplace injuries. As such,

the grantee's safety-related responsibilities may be numerous. They may include, for example:

- investigating major incidents
- identifying workplace hazards
- proper handling of hazardous materials
- emergency preparedness

An organization's safety culture is a reflection of the perceptions and values that all employees share regarding safety. This concept has a direct, measureable relationship to organizational performance and efficiency. However, promoting and maintaining a vibrant transit safety culture depends in part on employees believing that they are free to report hazards without punishment, or reprisals from management, as well as an expectation that those hazards will be resolved in a reasonable time frame.

Reviewers should ensure that the grantee has established procedures to investigate, identify, and address safety issues. The process should be both reactive in terms of investigating incidents and proactive in terms of identifying and responding to key safety issues and potential hazardous conditions.

REFERENCE
None

SOURCES OF INFORMATION
The minutes from safety committee and/or accident/incident review committee meetings should be made available during the site visit, as well as emergency management plans and procedures. The reviewer will examine safety statistics for the past three years for major incidents involving passengers, property damage, and work-related accidents. At the site visit or the desk review, the reviewer will examine newspaper articles or other publications describing accidents or safety incidents. This does not necessarily indicate poor safety practices; however, the incidents may be discussed at the site visit. Insurance companies also conduct assessments of their clients. Such reports are another source of information. Claims records and insurance costs identified in financial reports also provide information related to both costs and the actual number of incidents.

Procedures manuals and employee handbooks may contain information related to safety. The reviewer will examine copies of these documents on site to determine if safety procedures are addressed for various functions (e.g., transportation, maintenance, procurement, and storage). The reviewer will also determine who is responsible for maintaining safety information, handbooks, procedures manuals, and materials safety data sheets (MSDS).

DETERMINATION
If incident and accident investigation procedures appear to be lacking, an advisory comment is made.

If key safety issues, hazard identification or resolution procedures are lacking, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to develop and implement adequate procedures for investigating incidents.

The grantee will be advised to establish appropriate procedures for addressing key safety issues, workplace hazards, safe materials handling, etc.

7. *Do the grantee's policies address the use of cell phones and other personal electronic devices by safety critical personnel?*

EXPLANATION
In a Dear Colleague Letter dated June 26, 2009, FTA noted the role that texting and cell phone use by personnel has played in public transportation accidents. Through this letter, the Administrator urged transit operators to review policies, procedures, and enforcement mechanisms targeting the inappropriate use of cell phones and other personal electronic devices by safety critical personnel.

REFERENCE
FTA Dear Colleague Letter June 26, 2009

SOURCES OF INFORMATION
The reviewer will ask the grantee to provide information on how and when a review of personnel policies was performed in light of this Dear Colleague Letter. Policies, procedures, and enforcement mechanisms also will be examined.

DETERMINATION
If there is no evidence that the agency has policies, procedures or enforcement mechanisms regarding the use of personal electronic devices, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to develop and promulgate a policy governing the use of personal electronic devices.

8. *Does management hold line personnel accountable for safety? Do line personnel job descriptions (senior level to first-line supervisors) include a*

provision for safety accountability? Are safety responsibilities clearly defined? Do performance evaluations include an appraisal of safety performance?

9. *Is there safety training for employees performing safety sensitive functions? Who performs the training? How is it done? Do supervisors receive formal safety training?*

EXPLANATION
Grantees are encouraged to clearly define the safety responsibilities for all employees and establish a comprehensive safety training program. By providing training to the appropriate personnel, grantees can enhance safety performance in all areas (e.g., accidents, workplace hazards, and emergency preparedness). Training may consist of initial training to new hires as well as recurrent training to all employees. Additional training may be provided on a case-by-case basis, if employees have a high number of incidents in a particular area of concern.

REFERENCE
None

SOURCES OF INFORMATION
The reviewer will ask the grantee to provide an overview of its training program for drivers, mechanics, supervisors, and other line personnel. The reviewer will discuss job descriptions and requirements for safety sensitive positions and supervisory personnel and review employee training records (line personnel and supervisors). During the site visit, the grantee should make available training manuals, safety handouts, safety postings and other materials.

DETERMINATION
If safety responsibilities have not been clearly defined for safety-sensitive and supervisory personnel, an advisory comment is made.

If safety-sensitive and supervisory personnel have not received adequate safety training, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to clearly define safety responsibilities.

The grantee will be advised to develop an adequate safety training program.

10. *If the grantee operates rail service, and uses audio frequency track*

circuits in its train control system, has it implemented recommendations from the September 22, 2009, Dear Colleague Letter?

EXPLANATION
The FTA Administrator's Dear Colleague Letter related the National Transportation Safety Board's (NTSB) recommendations pertaining to rail transit operators that use audio frequency track circuits in their train control systems. FTA immediately advised all the pertinent operators to examine track circuits that may be susceptible to parasitic oscillation and spurious signals capable of exploiting unintended signal paths and eliminate those adverse conditions. Failing to do so could affect the safe performance of train control systems. This work should be conducted in coordination with signal and train control equipment manufacturers.

FTA will provide further direction shortly regarding the need for the same universe of operators to develop a program to periodically determine that electronic components in their train control systems are performing within design tolerances.

REFERENCE
FTA Dear Colleague Letter September 22, 2009

SOURCES OF INFORMATION
The reviewer will ask the grantee to provide information demonstrating that this examination has been done.

DETERMINATION
If recommendations from the Dear Colleague Letter have not been implemented, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to implement the recommendations from the Dear Colleague Letter of September 22, 2009.

11. *If the grantee operates rail service, and has train control systems capable of monitoring train movements, has it implemented recommendations from the July 14, 2009, Dear Colleague Letter?*

EXPLANATION
The FTA Administrator's Dear Colleague Letter related the NTSB's recommendations pertaining to rail transit operators that have train control systems capable of monitoring train movements. The letter

advised these operators to determine whether their systems have adequate safety redundancy if losses in train detection occur. If a system is susceptible to single point failure, operators were urged to take corrective action immediately to add redundancy by evaluating track occupancy data on a real-time basis to automatically generate alerts and speed restrictions to prevent train collisions.

REFERENCE
FTA Dear Colleague Letter July 14, 2009

SOURCES OF INFORMATION
The reviewer will ask the grantee to provide information demonstrating that this examination has been done.

DETERMINATION
If recommendations from the Dear Colleague Letter have not been implemented, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to implement the recommendations from the Dear Colleague Letter of July 14, 2009.

Part B. Security and Emergency Management

12. *Does the grantee utilize one percent of its Section 5307 expenditures for transit security? If yes, how were the funds utilized over the last three years? If no, how do existing security measures meet agency needs?*

EXPLANATION
The grantee is required to certify that it is spending at least one percent of the Section 5307 funds it receives annually for transit security projects or that such expenditures are not necessary. This certification is part of the annual certifications and assurances.

For grantees that spend the one percent, examples of appropriate security expenditures include facility perimeter security and access control systems (e.g., fencing, lighting, gates, card reader systems, etc.), closed circuit television camera systems (at stations, platforms, bus stops, and on-board vehicles), security and emergency management planning, training and drills (SAFETEA-LU expanded the definition of security related capital projects to include planning, training, and drills, such that these expenditures are now eligible expenses for grantees in UZAs over 200,000 population to apply towards the one percent

for security requirement), and any other project intended to increase the security and emergency management of an existing or planned transit system. Grantees should provide details on how these funds were spent during the review period.

There are three reasons that grantees may have for considering the one percent security expenditure to be unnecessary: (1) a recent threat and vulnerability assessment identified no deficiencies; (2) TSA/FTA Security and Emergency Management Action Items met or exceeded; or (3) other. For the "other" category, the typical reason is that a grantee spends sufficient local, or other FTA, Department of Homeland Security (DHS) funds on security projects and, therefore, does not need to spend formula grant funds on security projects. Regardless of the reasons for deciding not to spend Section 5307 funds on transit-related security, grantees should provide information and documentation that supports their decision.

REFERENCE
49 USC 5302(a)(1) and 5307(d)(1)(J)

SOURCES OF INFORMATION
The reviewer will examined security expenditure information in TEAM-Web. During the site visit, the reviewer will ask these questions. If a grantee is spending at least one percent of its formula funds on security projects, the grantee must detail these expenditures for each year of the review period in the requested format, as well as provide documentation that supports these expenditures.

If the grantee has decided that it is not necessary to expend one percent of its Section 5307 funds, it should provide a written explanation and any information that supports the decision. Such information may include the recommendations/ findings from a threat and vulnerability assessment or a TSA/FTA Security and Emergency Management Action Items assessment, such as a TSA *Baseline Assessment and Security Enhancement* (BASE) review. If the grantee indicates that it spends local funds on security, it should provide expense detail and documentation to support the amounts of these expenditures.

DETERMINATION
The grantee is deficient if it decides that expenditures for security are necessary but falls short of the one percent requirement.

The grantee is deficient if it cannot provide adequate documentation of its Section 5307 security expenditures.

The grantee is deficient if it decides that expenditures for security are not necessary but cannot explain or

provide adequate documentation to support its decision.

SUGGESTED CORRECTIVE ACTION
The grantee will be directed to submit to the FTA regional office a plan for meeting the one percent expenditure requirement and report on implementation of this plan.

The grantee will be directed to submit to the FTA regional office a plan for documenting the amount of formula funds spent on transit security.

The grantee will be directed to submit to the FTA regional office an explanation and adequate documentation on why the expenditure is not necessary.

13. *Has the grantee received a TSA BASE review within the last 12 months and scored at least 80 percent? If yes, skip remaining questions.*

EXPLANATION
TSA conducts BASE reviews of the top 100 transit agencies. The BASE review was developed from the FTA/TSA Security and Emergency Management Recommended Action Items for Transit Agencies. As such, TSA BASE review results can be utilized for the purposes of the security portion of the FTA Triennial Review, thus obviating the need to repeat the same set of questions.

REFERENCE
TSA BASE Program

SOURCES OF INFORMATION
The reviewer will ask this question of the grantee and examine the grantee's BASE review results as applicable.

DETERMINATION
Input into remaining questions.

SUGGESTED CORRECTIVE ACTION
None

14. *Does the grantee have written security and emergency management plans for all modes of operation?*

15. *Do the security and emergency management plans define roles and responsibilities for transit personnel?*

16. *Do the security and emergency management plans ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control?*

EXPLANATION
FTA has specific requirements for a written system security plan for rail fixed guideway systems (RFGS). FTA encourages all transit systems, particularly those in areas with populations of 200,000 or more, to develop and implement a transit system security program plan and emergency management plan that covers passengers, employees, vehicles, and facilities, including the planning, design, and construction of new facilities. Guidance on the development and implementation of system security program plans is available in a report entitled, *The Public Transportation System Security and Emergency Preparedness Planning Guide* (DOT-VNTSC-FTA-03-01), dated January 2003.

Grantees should ensure that security and emergency management plans are endorsed by senior level management in order that they are communicated throughout the agency from the highest level. Plans should be reviewed annually and updated as circumstances warrant. Plans should integrate visibility, randomness, and unpredictability into security deployment activities in order to avoid exploitable patterns and to enhance deterrent effects. Plans should also address continuity of operations and business recovery in the event that normal operations need to be suspended or altered as the result of a catastrophic incident. In addition, plans and protocols should address specific threats from improvised explosive devices, weapons of mass destruction, and other high consequence risks identified in transit risk assessments. Grantees should also establish and maintain standard security and emergency operations procedures (SOPs/EOPs) for each mode operated, including procedures for operations control centers.

In situations where grantees are planning the construction or modification of systems and facilities, security design and crime prevention criteria through environmental design (CPTED) should be applied to ensure a secure environment for the riding public and employees.

The security and emergency management programs should be assigned to senior level managers. The names and titles of the primary and alternate security coordinator (including security directors and transit police chiefs) should be recorded and maintained on file. The telephone numbers, e-mail addresses, and other contact information for these individuals should be accurately maintained so that they are accessible

at all times. Security coordinators also should report to senior level management. Security duties should be defined and properly delegated to front line employees.

The grantee should distribute the security and emergency management plans to appropriate personnel. Regular security coordination meetings involving all personnel assigned security responsibilities should be held. Informational briefings with appropriate personnel also should be held whenever security protocols are substantially updated. In order to ensure continuity of the plans, the grantee should establish lines of delegated authority and/or succession of security responsibilities and inform the affected personnel.

The grantee should hold regular supervisor and foreperson security review and coordination briefings for operations and maintenance personnel. An internal security incident reporting system should be developed and maintained and a security review committee should be established in order to regularly review security incident reports, trends, and program audit findings, and recommend changes to plans and processes to senior level management.

REFERENCE
49 CFR 659.31
TSA/FTA Action Item No. 1
TSA/FTA Action Item No. 2
TSA/FTA Action Item No. 3
The Public Transportation System Security and Emergency Preparedness Planning Guide

SOURCES OF INFORMATION
During the site visit, written security and emergency management plans will be examined. At the desk review or site visit, newspaper articles or other publications describing security incidents may be examined. Such articles may highlight an incident. Though this does not necessarily indicate poor security practices, the reviewer may discuss the incident at the site visit.

The security and emergency management plans may not be stand-alone documents, but may be chapters or sections of a more comprehensive safety/security plan, such as a system safety program plan for a rail fixed guideway system. The plan should cover all modes operated, including contracted services.

Note: Due to the sensitive security information designation of grantees' security and emergency management plans, they must be examined on site. Reviewers will not remove security and emergency management plans from the grantee's premises or request them in advance of the review.

DETERMINATION
If a grantee does not have a security plan for all modes, an advisory comment is made.

If a grantee has a security plan for each mode, but it does not include personnel roles and responsibilities, protocols to address specific threats, a continuity of operations, a business recovery plan, or other elements described in the explanation, an advisory comment is made.

If the plans do not have an endorsement from the top official, an advisory comment is made.

If responsibilities have not been clearly defined, an advisory comment is made.

If the grantee does not have an emergency management plan or if the plan does not cover all modes, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to prepare and implement a written security and emergency management plan for all modes.

The grantee will be advised to update its plan to address items noted in the Explanation section above.

17. *Are the security and emergency management plans coordinated with local agencies?*

EXPLANATION
A grantee's security and emergency management plans should be an integrated system and be coordinated with local first responders. Coordination should include mutual aid agreements with these agencies and should address communications interoperability with first responders (e.g., police and fire departments) in the grantee's service area. Grantees also should coordinate with Federal and state entities associated with public transportation security such as the TSA's Surface Transportation Security Inspection Program (STSIP) area office, the FBI's Joint Terrorism Task Force, the State Homeland Security Office, and FTA regional office. Coordinated plans should be consistent with the National Incident Management System (NIMS) and the National Response Framework (NRF). NIMS provides a unified approach to incident management, including standard command and management structures and an emphasis on preparedness, mutual aid, and resource management. The NRF forms the basis of how the Federal government coordinates with state, local, and tribal governments and the private sector during incidents.

REFERENCE
TSA/FTA Action Item No. 4
National Incident Management System
National Response Framework

SOURCES OF INFORMATION
The reviewer will ask the grantee to provide copies of security plans and procedures. Also, the reviewer will ask the grantee to provide copies of any inter-agency agreements that outline a coordinated emergency response. If no formal agreements exist, the grantee will be asked if it has met with representatives of other agencies to discuss and/or plan emergency response coordination. The grantee's plans should be consistent with NIMS and the NRF.

DETERMINATION
If the grantee has not coordinated with other agencies, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to coordinate with other local, state, and Federal agencies. The grantee will be advised to contact other agencies and begin developing coordinated emergency response procedures.

18. *Has the grantee established a security and emergency training program?*

EXPLANATION
The grantee should provide ongoing basic training to all employees in security orientation and awareness and emergency response. Ongoing training should be provided to employees that have direct security responsibilities such as operating, maintenance, law enforcement and fare inspection. Ongoing training should include advanced security and emergency response by job function and actions required at incremental Homeland Security Advisory System (HSAS) threat advisory levels. Security training programs should emphasize integration of visible deterrence, randomness, and unpredictability into security deployment activities to avoid exploitable patterns and heighten deterrent effect.

Advanced security training programs also should be established for transit managers, including but not limited to CEOs, general managers, operations managers, and security coordinators (includes security directors and transit police chiefs). The materials should be updated regularly to address high consequence risks that have been identified by the grantee's risk assessments. Training should reinforce roles and responsibilities and should ensure that employees are proficient in their duties at all times.

The grantee should establish a system that records personnel training in security and emergency response that, at a minimum, documents employees' initial training, and any recurrent training (e.g., periodic and/or refresher). Grantees should also establish and maintain a security notification process to inform personnel of significant updates to security and emergency management plans and procedures, as necessary.

REFERENCE
TSA/FTA Action Item No. 5

SOURCES OF INFORMATION
Procedure manuals, employee handbooks, and training materials may provide information on the grantee's efforts to train employees in security and emergency response. The reviewer will ask the grantee if security training seminars or workshops have been conducted for all employees and whether records are kept concerning security and emergency training. If so, a sample of these documents may be examined to verify the grantee's recordkeeping system. The reviewer will ask whether or not the grantee has a notification process to inform employees of significant updates to plans and procedures.

DETERMINATION
If training has not been provided to operating personnel, an advisory comment is made.

If training has not been provided to non-operating personnel, an advisory comment is made.

If the grantee does not maintain security training records, an advisory comment is made.

If the grantee does not have a process for providing employees with security and emergency plan updates, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to implement a security and emergency response training program for operating and/or non-operating personnel and maintain records of employee training.

The grantee will be advised to establish and maintain a notification process to inform employees of updates to security and emergency plans and procedures.

19. *Has the grantee established a risk management process to assess and manage threats, vulnerabilities, and consequences? Did the process identify mitigation measures after the risk assessment had been completed?*

EXPLANATION
Grantees are encouraged to establish a risk management process that is based on a system-wide assessment of risks and obtain management approval of this process. As part of the process, grantees should ensure proper training of management and staff responsible for managing the risk assessments. Whenever a new asset/facility is added or modified, and when conditions warrant (e.g., changes in threats or intelligence), the risk assessment process should be updated. The risk assessment process should be used to prioritize security investments.

As with the overall security and emergency management plans, the risk assessment process should be coordinated with regional security partners, including Federal, state, and local governments as well as agencies with shared infrastructure (e.g., other transit agencies or rail systems). Coordination will assist grantees to leverage resources and experience for conducting risk assessments.

REFERENCE
TSA/FTA Action Item No. 9

SOURCES OF INFORMATION
The reviewer will ask the grantee if it has established a risk assessment process and to provide documentation (e.g., risk assessments and mitigation measures) that demonstrates such a process has been established.

DETERMINATION
If the grantee has not established a risk management process, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to establish a risk management process and conduct risk assessments according to the established process.

20. *Are ID badges used for all visitors, employees, and contractors to control access to key critical facilities?*

21. *Has the grantee conducted a physical inspection of facilities to ensure that access is controlled and that facilities are secure?*

EXPLANATION
Grantees should identify security critical facilities and assets and ensure that access to these facilities is controlled. Grantees should develop written procedures to control access to security critical facilities and areas. The use of ID badges, while not required, is encouraged, for employees, visitors, and contractors that need entry to controlled areas. As with all policies and procedures, access control procedures should be updated as conditions warrant (e.g., new threats are identified).

Grantees should conduct, monitor, and document facility security inspections (e.g., perimeter/access control) on a regular basis. The frequency of such inspections should increase in response to elevation of the Homeland Security Advisory System (HSAS) threat advisory level. In addition, grantees should develop and use protocols for vehicle (e.g., buses and rail cars) inspections as well as protocols for inspections of rights-of-way corresponding to HSAS threat advisory levels. In order to integrate unpredictability in the process, grantees should vary the manner in which inspections of facilities, vehicles, and rights-of-way are conducted to avoid setting discernible and exploitable patterns.

REFERENCE
TSA/FTA Action Item No. 12
TSA/FTA Action Item No. 13

SOURCES OF INFORMATION
The grantee's policies and procedures that pertain to granting access to security critical systems and facilities will be examined.

DETERMINATION
If the grantee does not have policies and procedures for granting and reviewing access to security critical systems and facilities, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to develop procedures for access control for security critical systems and facilities.

22. *Have background investigations been conducted on all new front-line operations and maintenance employees?*

23. *Have criteria for background investigations been established?*

EXPLANATION
Operating personnel have a responsibility for the safety of the public that they serve. As such, it is imperative that grantees take all available precautions

in the hiring process to ensure the public's safety and security. Criminal background checks can be used to identify individuals that may pose a potential threat to the public safety and security. Although the focus of background checks is on new hires, grantees are encouraged to conduct checks for all operating employees, particularly those with access to safety and/or security critical systems (e.g., revenue vehicle operations and maintenance, signal rooms, and control centers). Grantees should establish specific criteria for background checks by employee type (e.g., operators, maintenance personnel, safety/security sensitive, and contractors). These criteria should be documented.

REFERENCE
TSA/FTA Action Item No. 14

SOURCES OF INFORMATION
The reviewer will ask the grantee if criminal background checks are performed on applicants for operating positions. If available, the reviewer will examine recent job applications (blank) or descriptions of application requirements. An individual's criminal background information is strictly confidential. Under no circumstances should a reviewer request to see individual records. Answers to these questions should be discussed in general terms within the context of the grantee's hiring practices.

DETERMINATION
If criminal background checks are not conducted for new hires, an advisory comment is made. If the grantee conducts background checks for new hires, but has not done so for existing employees, no advisory comment is made. However, grantees should be encouraged to check the criminal backgrounds of all operating employees, particularly those with access to safety and/or security critical systems.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to implement a program to conduct criminal background checks on all applicants for operating positions and for existing operating employees moving into any safety/security sensitive operations/maintenance positions, consistent with existing terms of labor agreements.

Questions 24 through 30 are applicable to grantees in a UZA of 200,000 or more.

24. *Have protocols been established to respond to HSAS threat advisory levels?*

EXPLANATION
FTA recommends that all grantees have an updated security plan that addresses terrorism, as well as procedures to respond incrementally to HSAS threat advisory levels issued by DHS.

REFERENCE
TSA/FTA Action Item No. 6

SOURCES OF INFORMATION
The reviewer will examine the grantee's security plan and/or procedures to ensure that there are protocols for responding to HSAS threat advisory levels.

DETERMINATION
If the grantee does not have protocols for responding to HSAS threat advisory levels, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to develop protocols to respond to HSAS threat advisory levels.

25. *Have public awareness materials been developed and distributed on a system-wide basis?*

EXPLANATION
The grantee should disseminate information to the riding public on identifying and reporting suspicious or illegal activity. Public service announcements, billboards, and brochures are effective mechanisms to provide security information to passengers. Grantees also should consider implementing FTA's Transit Watch program at their agency.

REFERENCE
TSA/FTA Action Item No. 7
Transit Watch

SOURCES OF INFORMATION
The reviewer will ask the grantee to provide any information related to security that has been disseminated to passengers.

DETERMINATION
If security information has not been provided to passengers, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to provide the riding public information on recognizing and reporting suspicious or illegal activity.

26. *Are tabletop and functional drills conducted at least once every six months, and are full-scale exercises, coordinated with regional emergency*

response providers, performed at least annually?

EXPLANATION
It is good practice for grantees to conduct tabletop exercises on a semi-annual basis and full scale exercises on an annual basis. Such drills and exercises should be coordinated with regional security partners, including Federal, state, and local governmental representatives and other affected entities (e.g., other transit agencies or rail systems) to integrate their representatives into exercise programs. Recommended exercise plans and procedures include threat scenarios involving improvised explosive devices, weapons of mass destruction, and other high consequence risks identified through the grantee's risk assessments. Following each exercise and drill, the grantee should conduct and/or participate in de-briefings to examine the results of the exercise and/or drill and develop after-action reports to address any updates to plans and procedures that might be warranted.

REFERENCE
TSA/FTA Action Item No. 8

SOURCES OF INFORMATION
The reviewer will ask the grantee what drills and/or exercises have been conducted. Ask the grantee to provide a list of the drills and exercises showing the dates that they were conducted and the other agencies that participated. The reviewer will examined any after-action reports and determine if plans and/or procedures were updated accordingly.

DETERMINATION
If the grantee has not conducted emergency drills and/or exercises, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to conduct and/or participate in coordinated emergency tabletop exercises on a semi-annual basis and full scale emergency exercises on an annual basis. The grantee will be advised to conduct or prepare de-briefings and/or after-action reports to address the results of the exercises and any updates to plans and procedures that might be warranted.

27. *Does the grantee participate in information sharing networks such as the FBI's Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force and/or the Public Transportation Intelligence Sharing and Analysis Center (PT-ISAC)?*

EXPLANATION
Grantees are encouraged to participate in intelligence sharing networks such as the FBI's JTTF (if they have their own law enforcement personnel) or PT-ISAC in order to facilitate coordination on regional security matters throughout the area and share intelligence with law enforcement and other agencies. PT-ISAC is a clearinghouse of security threats, vulnerabilities, and solutions for the public transit industry. Members report and receive information through the PT-ISAC to assist them and other members in preparing for and responding to threats. APTA is the coordinator for PT-ISAC. Other intelligence sharing networks include the DHS Homeland Security Information Network (HSIN) and the TSA's surface transportation security inspectors.

REFERENCE
TSA/FTA Action Item No. 10

SOURCES OF INFORMATION
The reviewer will ask the grantee if it participates in an information sharing network such as JTTF, PT-ISAC, or other agency to share intelligence on potential threats.

DETERMINATION
If the grantee does not participate in an information sharing network, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to join JTTF, ST-ISAC, or other regional task force in order to share intelligence on potential threats.

28. *Is access to documents of security critical systems and facilities controlled?*

29. *Does the grantee have a process for handling of and access to sensitive security information (SSI)?*

EXPLANATION
Controlling access to documents of security critical systems safeguards the public, transit employees, and transit assets from potential sabotage and security risks. Grantees should ensure that an appropriate level of security is provided around the plans and designs of its operating and maintenance facilities and its infrastructure (e.g., tunnels, bridges, electrical substations, etc.). Also, measures to protect documentation for security detection systems should be tightly controlled. The grantee should develop document control procedures to ensure that such documents are identified and that a person or department is made responsible for administering the document control program.

REFERENCE
TSA/FTA Action Item No. 15
TSA/FTA Action Item No. 16

SOURCES OF INFORMATION
The reviewer will ask the grantee if there are adequate document control procedures to safeguard SSI and documentation of security critical systems. Review policies and procedures.

DETERMINATION
If the grantee does not have procedures to control access to documentation of security critical systems and facilities and security sensitive documents, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to develop procedures to control access to documentation for security critical systems and facilities and security sensitive documents.

30. *Has the grantee conducted periodic audits of security policies and procedures?*

EXPLANATION
It is important for grantees to audit security and emergency response procedures and to take all necessary steps to identify potential security and emergency events. In determining the likelihood of security and emergency scenarios, a grantee can take actions to reduce the chances of an event occurring or, at a minimum, lessen its effects. For example, identifying fire hazards and implementing measures to address them can reduce or even eliminate the risk of fires from potential sources. Some events, such as natural disasters, are not preventable. However, with proper planning, the effects of these events can be mitigated.

REFERENCE
TSA/FTA Action Item No. 17

SOURCES OF INFORMATION
The reviewer will ask the grantee what audits have been conducted and examined any reports or memoranda that contain security audit information. The reviewer may examined security committee meeting minutes, if available. Procedures and plans should be updated to reflect findings from security audits.

DETERMINATION
If the grantee has not conducted an audit of its security policies and procedures, an advisory comment is made.

SUGGESTED CORRECTIVE ACTION
The grantee will be advised to audit its security and emergency response plans and to update plans and procedures as necessary.

EXHIBIT 19-1
TRANSIT SECURITY EXPENDITURES

Security Funding	FTA Section 5307 Funds		
	FY 2008	FY 2009	FY 2010
Total amount of 5307 funds expended			
Amount of 5307 funds expended on security			
Percent of 5307 funds expended on security			
Infrastructure/Capital Improvement Security Projects:			
Lighting, fencing & perimeter control			
CCTV and surveillance technology			
Communications systems			
Security planning			
Drills & tabletop exercises			
Employee security training			
Other security-related infrastructure & capital improvements (please list)			
Operating/Personnel Expenditures (for agencies in areas with populations under 200,000):			
Contracted security force			
In-house security force			
Other security-related operating expenditures (please list)			